REMARKS/ARGUMENTS

We thank the Examiner for the detailed comments. The Office Action has been carefully considered. It is respectfully submitted that the issues raised are traversed, being hereinafter addressed with reference to the relevant headings appearing in the Detailed Action section of the Advisory Action.

Claim Rejections – 35 USC § 103

At page 3 of the Office Action, the Examiner rejects claims 1 to 16 as being unpatentable over Shigenaga (US Patent No. 4,710,613).

The Applicant has also amended claim 1 and 7 to further clarify that the method and system relate to determining whether the consumable can be consumed by the consuming device. Support for this amendment can be found generally on page 31 of the specification as well as other areas of the specification relating to authenticating whether the consumable can be validly consumed.

Reconsideration and withdrawal of the claim rejection is respectfully requested in light of the below comments and claim amendments.

The Examiner has stated that although Shigenaga does not disclose the trusted authentication chip is contained within a consuming device, and the untrusted authentication chip is contained within the consumable, Shigenaga is an analogous art and therefore the claims are obvious in view of Shigenaga.

The MPEP states at § 2141.01(a):

> *"In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned."* In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992).

The Applicant submits that Shigenaga is not in the field of the applicant's endeavor, and furthermore, Shigenaga is not reasonably pertinent to the particular problem with which the inventor was concerned.

In regard to the first question (field of applicant's endevor), the Shigenaga citation involves an Intergrated Circuit card which is identified by an Integrated Circuit Terminal using a specific algorithm relating to encryption and estimated processing times. The Shigenaga citation can hardly be considered by the Examiner as being in the field of the applicant's endeavor when the applicant's method and system relate to authenticating whether a consumable containing an untrusted chip can be consumed by a consuming device containing a trusted chip. There is absolutely no reference to consumables in the Shigenaga citation and surely this must indicate to the Examiner that the Shigenaga citation cannot be considered to be in the field of applicant's endeavor. Thus, the Applicant respectfully submits that the answer to the first question should be answered in the negative by the Examiner.

In regard to the second question (reasonably pertinent to the particular problem with which the inventor was concerned), the problem which the applicant is attempting to solve is to ensure that a consumable which was not validly manufactured for the consuming device would not be consumed by the consuming device, and that only a valid consumable would be consumed by the consuming device. If a non-valid consumable is used with the consuming device, problems associated with the consumable malfunctioning can lead to the consuming device also malfunctioning. This can also lead to warranty claims related to the consuming device when actually it was the consumable which caused the problem. We note that these problems are highlighted in the introductory portion of the specification. Prior solutions have involved using unique packaging to deter other manufacturers developing generic consumables which could also operate with the consuming device.

The Shigenaga citation is not pertinent to the field of consumables which the applicant's system is designed for. The Shigenaga citation discloses a system used for restricting access to confidential information stored in the IC card using estimated processing time comparisons. Furthermore, the Shigenaga citation is concerned with indentifying the card holder of the IC card.

In contrast, the Applicant's system and method relates to determining whether a consumable can be consumed by a consuming device containing authentication chips. The authentication

chips allow the system and consuming device to determine whether the consumable is able to be consumed by the consuming device.

The Applicant submits that based on these facts, there is very little to suggest that the Shigenaga citation is pertinent to the field of authenticating consumables. The Shigenaga citation would not logically have commended itself to an inventor's attention in considering his problem relating to authenticating whether a consumable is valid for the particular consuming device, and thus can or cannot be consumed by the consuming device. Thus, the Applicant respectfully submits that the answer to the second question should be answered in the negative by the Examiner.

As the Applicant has respectfully submitted that both questions should be answered in the negative, the Applicant respectfully submits that the Shigenaga should not be considered analogous art. Furthermore, the Applicant respectfully directs the Examiner's attention to the decision in *Wang Laboratories, Inc. v. Toshiba Corp.*, 993 F.2d 858, 26 USPQ2d 1767 (Fed. Cir. 1993). The facts in this case share a striking resemblance to the current case, and as such the Applicant submits that the Examiner should similarly consider the claims as nonobvious in light of Shigenaga.

The Applicant has also included new claims 17, 18 and 19 to specify further distinctions over Shigenaga.

In particular, claim 17 is directed towards a processing system which transfers a request to the trusted chip to generate an original number, receives the original random number and the encrypted random number from the trusted chip, transfers the random number to the untrusted chip, receives the decrypted random number from the untrusted chip, and compares the original random number with the unencrypted random number. Support for these amendments can be found on page 39 of the specification and Figure 4.

Shigenaga fails to show a processing system which is configured to perform the above mentioned functionality. In particular, Shigenaga only discloses the IC terminal unit and the IC Card. Shigenaga fails to show a cental system which receives both the original random number and the encrypted random number. By providing a processing system which receives both the random number and the encrypted number, the processing system need not know

the secret key of the untrusted chip as well as the public key of the trusted chip. Furthermore, the trusted chip can be provided with simplified circuitry to securely produce a random number and an encrypted random number. Thus, the trusted chip does not need to be provided with a comparison means in order to determine whether the untrusted chip is valid.

The applicant respectfully submits that there is no teaching or suggestion in Shigenaga that a processing system could be provided that could perform the claimed functionality. Shigenaga explicitly teaches that the identification system is constituted of a first unit and a second unit. Nowhere in Shigenaga is there disclosed, taught or suggested a third unit which could be used to perform the above claimed functionality of the processing system. As such the applicant respectfully submits that the claims, as currently amended, should be considered patentable over Shigenaga.

Claim 18 has been introduced to specify that the untrusted chip includes an electronic noise generator to emit electronic noise to restrict detection of processing performed within the untrusted chip. Support for this feature can be found at page 104 under the heading "Noise Generator".

The Applicant submits that Shigenaga fails to disclose an electronic noise generator, and therefore claim 18 is patentable in view of Shigenaga.

Claim 19 has also been introduced to specify that the untrusted chip includes a light emitting component operably connected to the electronic noise detector to emit light to restrict detection of processing performed within the untrusted chip. Support for this feature can be found at pages 108 and 109 under the heading "Special implementation of FETs for key data paths" in regard to CMOS inverters and non-Flashing CMOS components.

The Applicant submits that Shigenaga fails to disclose a light emitting component operably connected to the electronic noise detector to restrict detection of processing performed within the untrusted chip, and therefore claim 19 is patentable in view of Shigenaga.

Reconsideration and withdrawal of this rejection is respectfully requested in light of the above claim amendments and the above comments.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections. The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762